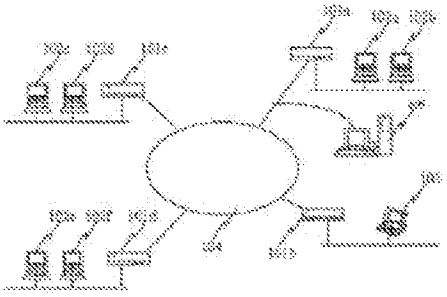
NETWORK SYSTEM

Publication number: JP9214493 (A)
Publication date: 1997-08-15
Inventor(s): TERADA MASATOSHI; YOSHIDA KENICHI; KAYASHIMA MAKOTO +
Applicant(s): HITACHI LTD +
Classification:
- International: ***G06F1/00; G06F11/30; G06F13/00; G06F15/00; G06F21/00; G06F21/20; H04L29/06;*** (IPC1-7): G06F11/30; G06F13/00; G06F15/00; H04L12/24; H04L12/28; H04L12/56
- European: G06F21/00N3P3; H04L29/06S14C
Application number: JP19960022781 19960208
Priority number(s): JP19960022781 19960208

Also published as:
US5831946 (A)

Abstract of **JP 9214493 (A)**

PROBLEM TO BE SOLVED: To provide a computer inspection system suitable for a large scale network. SOLUTION: A management equipment 103 distributes an external inspection program and an internal inspection program to routers 101 (101a-101d). The router 101 distributes the internal inspection program to computers 102 (102a-102f). When the inspection result of each computer 102 and obtained by executing the external inspection program and the result of the internal inspection according to the internal inspection program reported from each communication 102 indicate a fault, the router 101 commands collection of traffic log with respect to the computer 102 having the fault to a log collection device 105 and stops relay of a packet to the faulty computer 102.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－214493

(43)公開日　平成９年(1997)８月15日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ			技術表示箇所
Ｈ０４Ｌ	12/24		9466－5K	Ｈ０４Ｌ	11/08		
	12/26			Ｇ０６Ｆ	11/30	Ｅ	
Ｇ０６Ｆ	11/30				13/00	３５１Ｈ	
	13/00	３５１				３５３Ｕ	
		３５３			15/00	３２０Ｋ	

審査請求　未請求　請求項の数７　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願平8－22781

(22)出願日　平成８年(1996)２月８日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　寺田　真敏
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　吉田　健一
埼玉県比企郡鳩山町赤沼2520番地　株式会社日立製作所基礎研究所内

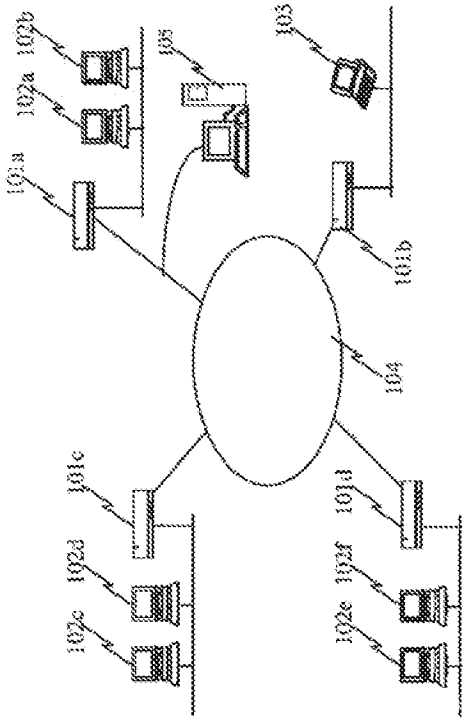
(72)発明者　釜島　僚
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　富田　和子

(54)【発明の名称】　ネットワークシステム

(57)【要約】
【課題】大規模ネットワークに好適な計算機の監査システムを提供する。
【解決手段】管理装置１０３は各ルータ１０１に外部監査プログラムと内部監査プログラムを配布する。ルータ１０１は各計算機１０２に内部監査プログラムを配布する。ルータ１０１は外部監査プログラムを実行して得た各計算機１０２の監査結果と計算機１０２から報告された組込部監査プログラムに従った内部監査結果に異常がある場合には、ログ収集装置１０５に、異常があった計算機１０２に関するトラフィックログの収集を指示する。また、異常があった計算機１０２へのパケットの中継を停止する。

図１



1

【特許請求の範囲】
【請求項１】ネットワークに接続した複数の計算機と、前記計算機間の通信の中継を行う複数の中継装置とを含むネットワークシステムであって、
前記ネットワークに接続した管理装置を備え、
前記管理装置は、各中継装置に、当該中継装置が他の中継装置を介さずに接続している計算機の稼動環境を前記中継装置が監査する外部監査処理の処理手順を規定する外部監査プログラムを前記ネットワークを介して配布する手段を有し、
前記中継装置は、前記管理装置から配布された外部監査プログラムに従って、前記外部監査処理を実行する手段を有することを特徴とするネットワークシステム。
【請求項２】請求項１記載のネットワークシステムであって、
前記管理装置は、各計算機に、計算機の稼動環境を当該計算機が自身で監査する内部監査処理の処理手順を規定する外部監査プログラムを前記ネットワークを介して配布する手段を有し、
前記計算機は、前記管理装置から配布された外部監査プログラムに従って、前記内部監査処理を実行する手段を有することを特徴とするネットワークシステム。
【請求項３】請求項２記載のネットワークシステムであって、
前記計算機は、前記内部監査処理の処理結果を、当該計算機が他の中継装置を介さずに接続している前記中継装置に報告する手段を有することを特徴とするネットワークシステム。
【請求項４】ネットワークに接続した複数の計算機と、前記計算機間の通信の中継を行う複数の中継装置とを含むネットワークシステムであって、
前記中継装置は、当該中継装置が他の中継装置を介さずに接続している計算機の稼動環境を監査する手段と、監査の結果、計算機の稼働環境が正規の環境と整合しない場合に、当該計算機への前記通信の中継を抑止する手段とを有することを特徴とするネットワークシステム。
【請求項５】ネットワークに接続した複数の計算機と、前記計算機間の通信の中継を行う複数の中継装置とを含むネットワークシステムであって、
ネットワークに接続し、ネットワーク上の通信の履歴を収集するログ収集装置を備え、
前記中継装置は、計算機の稼動環境を監査する手段と、監査の結果、計算機の稼働環境が正規の環境と整合しない場合に、稼働環境が正規の環境と整合しない計算機への通信の履歴の収集を、前記ネットワークを開始給前記ログ収集装置に指示する手段を有し、
前記ログ収集装置は、前記中継装置より指示に応じて、指示された計算機への通信の履歴を収集することを特徴とするネットワークシステム。
【請求項６】請求項５記載のネットワークシステムであって、

2

前記ログ収集装置には、ネットワーク上の通信の宛先として用いられるアドレスが与えられておらず、
前記ログ収集装置は、前記ネットワークの当該ログ収集装置の接続地点を通る全ての通信を監視し、通信が前記中継装置より指示である場合に、当該通信を受信することを特徴とするネットワークシステム。
【請求項７】ネットワークに接続した複数の計算機と、前記計算機間の通信の中継を行う複数の中継装置とを含むネットワークシステムであって、
前記中継装置は、計算機の稼動環境を監査する手段と、監査の結果、計算機の稼働環境が正規の環境と整合しない場合に、その旨を報知する手段を有することを特徴とするネットワークシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークに接続した計算機のセキュリティに関する技術に関し、特に計算機の稼動環境の監査や、監査結果に基づく不正な侵入者に対する防御の技術に関するものである。
【０００２】
【従来の技術】従来、ネットワークに接続した計算機の稼動環境の不整合を監査するシステムとしては、計算機内部から監査を実施し、計算機自身の稼動環境の不整合を計算機内部で検出する技術や、ネットワーク経由で所定の管理装置から計算機に稼動環境を問い合わせるパケットもしくはメッセージを送り、これに対する計算機の応答に基づいて管理装置において計算機の稼動環境の不整合を検出するシステムが知られている。
【０００３】ここで、計算機の稼動環境の不整合とは、本来、計算機中のファイル“a”の参照は、ユーザ“a“のみ可能であるべきものが、ユーザ”x“もファイル“a”を参照可能な状態に設定されている等の設定パラメタの不整合や、本来、計算機上のアプリケーションは、コマンド”xxx“は受け付けないにもかかわらず、コマンド“xxx“を受け付けてしまう等のアプリケーションの不具合などが挙げられる。
【０００４】なお、具体的には、計算機内部から計算機を監査する技術としてCOPS(Computerized Oracle and Password System)が、計算機外部の管理装置から監査する技術としてはSATAN(Security Administrator Tool for Analyzing Networks),ISS(Internet Security Scanner)が知られている。
【０００５】
【発明が解決しようとする課題】さて、現在では、インターネットなどのグローバルネットワークの発展により、世界の各地から発信された情報を手元の計算機でリアルタイムに入手できるようになった。しかし、その反面では、各計算機は外部からの侵入者の脅威にさらされることになった。

3

【０００６】このような侵入者に対する防御策として、計算機の稼動環境の不整合を監査し、これを修正しておくことは不正に計算機に侵入する足掛かりを少なくするという点で重要である。不整合な環境を保持したままの計算機が1台でもあると、これを足掛かりにして不整合な環境を保持した計算機周囲の計算機にまで不正に侵入される可能性が生じる場合すらある。

【０００７】したがって、監査結果に異常がある場合に効果的な対策をとることが必要となる。

【０００８】また、大規模なネットワークシステムを構築する場合には、管理装置と監査対象となる計算機との間で直接通信できる構成を採用できないことがある。そして、このような場合には、管理装置からの各計算機を集中的に監査することができなくなってしまう。

【０００９】そこで、本発明は、大規模なネットワークを対象とした計算機の監査システムを提供することを目的とする。また、計算機の稼動環境に不整合がある場合には、稼動環境の不整合を持つ計算機への不正な侵入を防止することを目的とする。

【００１０】

【課題を解決するための手段】前記目的達成のために、本発明は、たとえば、ネットワークに接続した複数の計算機と、前記計算機間の通信の中継を行う複数の中継装置とを含むネットワークシステムであって、前記ネットワークに接続した管理装置を備え、前記管理装置は、各中継装置に、当該中継装置が他の中継装置を介さずに接続している計算機の稼動環境を前記中継装置が監査する外部監査処理の処理手順を規定する外部監査プログラムを前記ネットワークを介して配布する手段を有し、前記中継装置は、前記管理装置から配布された外部監査プログラムに従って、前記外部監査処理を実行する手段を有することを特徴とするネットワークシステムを提供する。

【００１１】このようなネットワークシステムによれば、随時、管理装置から中継装置が実行する監査プログラムを最新、最良のものに更新することができる。また、各中継装置が監査処理の対象とする計算機を中継装置が直接（他の中継装置を介さずに）接続している計算機としているので、当該中継装置と当該計算機との間で必ず、直接通信することができる。また、計算機の監査のために生じる通信のトラフィックを低減することができる。従って、大規模ネットワークに好適な監査システムを実現することができる。

【００１２】また、本発明は、前記目的達成のために、たとえば、　ネットワークに接続した複数の計算機と、前記計算機間の通信の中継を行う複数の中継装置とを含むネットワークシステムであって、前記中継装置は、当該中継装置が他の中継装置を介さずに接続している計算機の稼動環境を監査する手段と、監査の結果、計算機の稼動環境が正規の環境と整合しない場合に、当該計算機への前記通信の中継を抑止する手段とを有することを特徴とするネットワークシステムを提供する。

4

【００１３】このようなネットワークシステムによれば、計算機の稼動環境が正規の環境と整合しない計算機への通信は、当該計算機には届かない。したがって、このような計算機への不正な侵入を防止することができる。

【００１４】

【発明の実施の形態】以下、本発明の一実施形態について説明する。

【００１５】図１に本実施形態に係るネットワークシステムの構成を示す。

【００１６】図中、１０３はネットワークシステムに接続した各計算機を集中的に監査するための管理装置である。１０１a～１０１dはTCP(Transmission Control Protocol)/IP(Internet Protocol)、OSI(Open Systems Interconnection)プロトコル等の所定の通信プロトコルに従った中継処理（ルーティング）を行う中継装置である。なお、本実施形態では中継装置の一例として、ルータを用いる。１０２a～１０２fは各ユーザサイトに設置されている計算機である。１０５はログ収集装置であり、各計算機からの処理のログや、ネットワーク上のトラフィックのログの収集を行う。

【００１７】なお、本実施形態では、各装置間のデータパケットの転送には、TCP(Transmission Control Protocol)/IP(Internet Protocol)、OSI(Open Systems Interconnection)等の転送機能を使用する。そして、各中継装置１０１a～１０１dは、データパケットの中継／廃棄を行うフィルタリング機能を備える。

【００１８】次に、図2に、ルータ１０１，管理装置１０３、ユーザサイトの計算機１０２、ログ収集装置１０５の一ハードウェア構成例を示す。

【００１９】図中、２０４はネットワークを構成するLAN、専用線などとの入出力を制御する回線制御部である。２０５はディスプレイ、キーボード２０６を制御する端末入出力制御部である。２０３はプログラムや、送受信メッセージを格納するメモリである。２０２はプロセサであり装置内の各部の制御を行う。回線制御部２０４が収容する回線数は、装置毎に異なる。計算機１０２、管理装置１０３であれば最小１つの回線を収容すればよく、ルータ１０１であればパケットの中継を行う最小2つの回線を収容すればよい。また、ログ収集装置であればトラフィックのログを収集する対象とする１以上の回線を収容するようにする。

【００２０】次に、図3にルータ１０１のソフトウェア構成を示す。

【００２１】図中、３０２はデータパケットの転送やフィルタリングを行うための中継制御情報の格納部（ルーティングテーブル）である。データ中継制御部３０３は中継制御情報に基づき、データパケットのフィルタリン

グや、目的とする計算機への転送を制御する。３０４はネットワークとの入出力や外部の入出力装置との入出力を制御する外部インタフェース制御部であり、回線制御部２０４、端末入出力制御部２０５に記憶されている。３０６～３０７は、内部ならびに外部監査プログラム群である。３０８は管理装置１０３から配布される最新の内部監査プログラム３０７ならびに外部監査プログラム３０６の受信や、配布された内部監査プログラム３０７の各計算機への配布を制御する監査プログラム配布・受信部である。監査制御部３０９は、監査結果に応じて異常の通知などの処理を行う。プログラムスケジューラ３０６は、３０１～３０９のプログラム実行のスケジューリングと管理を行う。

【００２２】次に、図４に、計算機１０２のソフトウェア構成を示す。

【００２３】図中、４０２はデータパケットを送受信するための経路情報であるデータ送受信制御情報を格納する格納部である。４０３はデータ送受信制御情報に基づき、目的とする計算機との間でデータパケットの送受信を行うで送受信制御部である。４０４は回線制御部２０４、端末入出力制御部２０５に設けられ、ネットワークとの入出力、外部の入出力装置との間の入出力を制御する外部インタフェース制御部である。０６a～４０６bは計算機上で稼動するアプリケーションである。４０７は内部監査プログラム、４０８はルータ１０１または、管理装置１０３から配布される内部監査プログラムの受信を行う監査プログラム受信部である。プログラムスケジューラ４０５は、４０２～４０８のプログラム実行のスケジューリングと管理を行う。

【００２４】次に、図５に、管理装置１０３のソフトウェア構成を示す。

【００２５】図中、５０２はデータパケットを送受信するための経路情報であるデータ送受信制御情報を格納する格納部である。５０３はデータ送受信制御情報に基づき、目的とする計算機との間でデータパケットの送受信を行うデータ送受信制御部である。５０４は回線制御部２０４、端末入出力制御部２０５に設けられ、ネットワークとの入出力、外部の入出力装置との間の入出力を制御する外部インタフェース制御部である。５０６はルータならびに各計算機に配布する監査プログラム群を、監査プログラムリストによって管理する管理部である。５０７は各ルータに最新の監査プログラムを配布するための監査プログラム配布部５０７である。プログラムスケジューラ５０５は、４０２～４０８のプログラム実行のスケジューリングと管理を行う。

【００２６】次に、図６に、ログ収集装置１０５のソフトウェア構成を示す。

【００２７】図中、１１０２はデータパケットを受信するための制御情報であるデータ受信制御情報の格納部である。１１０３はデータ受信制御情報に基づき、データパケットを受信するデータ受信制御部である。１１０４は回線制御部２０４、端末入出力制御部２０５に設けられ、ネットワークとの入出力、外部の入出力装置との間の入出力を制御する外部インタフェース制御部である。１１０６はログ情報を格納するログ情報格納部である。プログラムスケジューラ１１０５は、１１０２～１１０８のプログラム実行のスケジューリングと管理を行う。

【００２８】なお、本ログ収集装置１０５は、以下のような特徴を有している。

【００２９】(a)　図１に示すように、ネットワークを構成するLAN、専用線などの正規の接続線から分岐した分岐線に接続され、ネットワーク上に流れるデータを収集する。これは、ログ収集装置１０５は、ネットワーク上に流れるデータを第三者的に取り出すことを意味する。

【００３０】(b)　ログ収集装置１０５は、TCP/IP,OSI等で使用されるネットワークアドレスを持たない。従って、管理装置１０３、ルータ１０１、計算機１０２から、本ログ収集装置１０５を明示的に宛先指定してメッセージ，データパケットを送信することはできない。また、ログ収集装置１０５からも管理装置１０３、ルータ１０１，計算機１０２宛にメッセージを送信することはできない。

【００３１】これにより、ネットワークを介してログ収集装置１０５に侵入し、ログ収集装置１０５に格納されたログ情報の改竄や破壊を行うことは、極めて困難となる。

【００３２】さて、以上のような構成において、管理装置１０３は、外部監査プログラムと内部監査プログラムをネットワークを介して各ルータ１０１に配布する。さらに、各ルータ１０１は、管理装置１０３から配布された内部監査プログラムのうち計算機上で実行されるべき内部監査プログラムを各計算機１０２に配布する。ここでこのように、内部監査プログラムとしては、ルータ上で実行されるものと、計算機上で実行するものとがある。ルータ上で実行される内部監査プログラムは、計算機上で実行される内部監査プログラムの起動と、計算機上で実行される内部監査プログラムによる監査結果の検証を行う。

【００３３】以下、この内部／外部監査プログラムの配布の手順について説明する。

【００３４】図７に、内部／外部監査プログラムの配布のシーケンスを示す。

【００３５】図示するように、まず，管理装置１０３は、監査プログラム配布部５０６において最新の監査プログラムの一覧を作成し（６０１），これに従い、最新の内部／外部監査プログラムを、外部インタフェース制御部５０４より計算機の外部よりの監査を実施するルータ１０１に配布する（６０２）。ルータ１０２では，外部インタフェース制御部３０４で，これを受信する。そ

して、ルータ１０２の監査プログラム配布・受信部３０８は、自身が保有する内部／外部監査プログラム３０６、３０７を管理装置１０３より配布された内部／外部監査プログラムに更新すると共に、ユーザサイトの各計算機に配布する内部監査プログラムの一覧を作成後(６０３)、各計算機に内部監査プログラムを外部インタフェース制御部３０４を介して配布する(６０４)。各計算機１０２では、ルータ１０２よりの内部監査プログラムを外部インタフェース制御部４０４で受信する。そして、監査プログラム受信部４０８は、自身が保有する内部監査プログラム４０７の受信した内部監査プログラムへの更新を行う(６０５)。これにより、管理装置より、関連するルータ、計算機への最新の内部／外部監査プログラムの配布が終了する。

【００３６】なお、監査制御部３０９の行う処理のプログラムもが外部監査プログラムと共に管理装置１０３から配布し、ルータ１０１において逐次更新するようにしてもよい。また、内部／外部監査プログラムの配布そのものは、ファイル転送、ネットワーク管理システム、メール等のメッセージ転送機能を利用することができる。また、配布にあたって監査プログラム自身の盗聴を防ぐため共有鍵や公開鍵を用いたデータパケットの暗号化し、改竄を防ぐためプログラムに対してデジタル署名を付加し、正当な送信元と宛先計算機を特定するためユーザ名、パスワード等の認証機構を付加することにより、監査プログラムの配布においても安全性の向上を図ることができる。これらの安全性を向上する技術は、PEM(Privacy Enhanced Mail)、PGP(Pretty Good Privacy)、SNMP２(Simple Network Management Protocol ２)等において実現されている。

【００３７】さて、このようにして内部／外部監査プログラムが配布されると、ルータ１０１は配布された外部監査プログラムを実行することにより計算機の外部よりの監査を実行する。また、各計算機は、配布された内部監査プログラムを実行することにより内部からの監査を実行する。なお、各ルータ１０１には、当該ルータが外部プログラムに従って監査を行うべき計算機１０２、内部監査プログラムを配布すべき計算機として、直接（他のルータを介さずに）通信を行うことのできる計算機が割り当てられる。

【００３８】以下，各計算機の外部／内部よりの監査の手順について説明する。

【００３９】図８に、外部よりの監査のシーケンスを示す。

【００４０】図示するように、まず、プログラムスケジューラ３０５、監査制御部３０９の制御下で、外部監査プログラムの実行を開始したルータ１０１は、外部インタフェース制御部３０４を介して、外部よりの監査の対象とする計算機１０２上のアプリケーション４０６に対して監査パケット９０１を送信する。各計算機上のアプリケーション４０６は外部インタフェース制御部４０４を介して受信した監査パケットに応答して、アプリケーションプログラム自身が監査パケットに応答して行った動作結果を応答パケットとして外部インタフェース制御部４０４を介して、ルータ１０１に返送する(９０２,９０３)。監査パケットは、たとえば，アプリケーションプログラムの設定パラメータを要求するものであり、応答パケットは，アプリケーションプログラムの設定パラメータを送信するものである。

【００４１】ルータ１０１上の外部監査プログラムは、受信した応答パケットの内容と、外部監査プログラムに含まれる稼動環境の不整合がない場合の応答パケットの内容とを比較することにより，その計算機における稼動環境の不整合の有無を判断する(９０３)。

【００４２】このように、各ルータから各計算機の外部監査を実施することにより、何らかの都合で管理装置と監査対象となる計算機とが直接通信できない場合にも外部よりの監査を実現でき、管理装置から集中的に外部監査を実施する場合に比べ、ネットワーク全体として監査時のトラフィックを低減することができる。

【００４３】次に，図９に内部からの監査のシーケンスを示す。

【００４４】ルータ１０１において、プログラムスケジューラ３０５、監査制御部３０９の制御下で起動された内部監査プログラム３０７は、、監査の対象とする計算機１０２上の内部監査プログラム４０７に対して監査実施指示パケット１００１を送信する。すると、各計算機上のプログラムスケジューラ３０５は，自身が保有する内部監査プログラム４０７を起動し(１００３)する。起動された内部監査プログラム４０７は、内部からの監査を実施し、その結果を監査結果パケットとしてルータ１０１に返送する(１００２)。ルータ上の内部監査プログラム３０７は、受信した監査結果パケットの結果を確認することにより，その計算機における稼動環境の不整合の有無を監査する(１００４)。

【００４５】なお、内部／外部監査プログラムによって実現される監査の内容は、個々の計算機やネットワークが提供する機能などに応じて定めるべきものであり，多種多様な内容の監査が考えられる。

【００４６】ここで，図１０に、以上のような外部／内部よりの監査においてルータ１０１と計算機１０２との間でやりとりされる各パケットのフォーマットを示しておく。

【００４７】図１０は、パケットのフォーマットを示したものである。図示するように、これらのパケットは、３つのフィールドを含み，第１フィールドにはパケットの種別、第２フィールドには操作方法、第３フィールドには転送されるデータが格納される。

【００４８】外部よりの監査の際に用いられる監査ならびに監査応答パケット９０１は、図１０ (a) に示すよ

うに、パケットの種別を示す第１フィールドには「データ８０１a」，操作方法を示す第２フィールドには「mul 1802a」，転送されるデータである第３フィールドには計算機上のアプリケーションに送付するメッセージ８０３aが設定される。

【００４９】また、内部よりの監査の際に用いる監査実施指示パケット１００１の第１～第３フィールドには，図１０（b）に示すように、「監査８０１b」、「指示８０２b」、先に計算機に配布した内部監査プログラムであって、計算機上で起動させたい内部監査プログラムの一覧である「監査プログラム指示リスト８０３b」が設定される。また，監査結果パケット１００２の第１～第３フィールドには、図１０（c）に示すように「監査８０１c」、「結果８０２c」、計算機上で実行した内部監査プログラムの結果一覧である「監査結果８０３c」が設定される。

【００５０】このようにして、計算機の外部／内部よりの監査が終了すると，各ルータ１０１は、内部もしくは外部よりの監査の結果を検証し、検証結果に応じた処理を行う。

【００５１】すなわち、ルータ１１０１の監査制御部３０９は、図１１に示すように、自身が保有する外部監査プログラム、ルータ上で実行される内部監査プログラムを順次実行し（７０１）、これらのプログラムの実行により得られた計算機における稼動環境の不整合（異常）の有無を確認した結果、異常がある場合には（７０３）、監査結果を計算機管理者ならびに、システム全体を管理する管理者に通知する（７０４）。通知は、管理者が使用する計算機に異常を伝えるメッセージを含むパケットを外部インタフェース制御部３０４を介して送信し、メッセージを受けた計算機において当該メッセージを出力することなどにより行う。また、ログ収集装置に対して、監査結果に異常のある計算機へのトラフィックログの取得の開始を指示する。ログ収集装置１０５のデータ受信制御部１１０３は、この指示に従って、以降、当該計算機宛のパケットがログ情報格納部１１０６に蓄積していくように外部インタフェース制御部１１０４ログ情報格納部１１０６を制御する。収集されたトラフィックログは、稼動環境に不整合がある計算機へのアクセス状況の記録を残すことにより，外部からの不正アクセスの検証を行う等に使用することができる。また、このようなトラフィックログの収集には，不正なアクセスを試みる者への心理的な抑止効果が期待できる。なお、本実施形態ではまた、トラフィックログの収集を専用のログ収集装置により実施するため，データの中継装置として動作するルータのデータ転送性能を低下させることがない。

【００５２】次に、一定期間内に稼動環境に不整合がある計算機への対策がなされたことを表すメッセージを受信しなかった場合に、ルータの監査制御部３０９は、稼動環境に不整合がある計算機へのパケットの中継を停止させるパケットフィルタリングを設定し、稼動環境の不整合がある計算機を隔離し、計算機セキュリティを高める動作をとる。稼動環境に不整合がある計算機へのパケットの中継の停止は，ルータ１０１の格納部３０２の中継制御情報変更することにより実現する。なお、ルータ１０１において、稼動環境に不整合がある計算機からのパケットの中継も停止するようにしてもよい。

【００５３】ところで、稼動環境に不整合がある計算機への対策は、人手により稼動環境の不整合を排除する方法や、予め登録してある対策手順に基づき対処する方法，これまでの対策手順を学習した結果に基づき計算機自身が自己修復を実施する方法などを用いる。いずれの場合も、対策が終了したら、その旨を伝えるメッセージをルータ１０１に計算機より送信するようにする。

【００５４】一方，管理者に異常を通知してから一定期間内に対策が実施された旨のメッセージを受信した場合には、ログ収集装置１０５に対して、トラフィックログの取得の停止を指示する。ログ収集装置１０５のデータ受信制御部１１０３は，この指示に従って、外部インタフェース制御部１１０４ログ情報格納部１１０６を制御し、当該計算機あてのパケットの蓄積を停止する。

【００５５】なお，前述したように、ログ収集装置１０５はネットワークアドレスを与えられていない。そこで、ルータ１０１からのログ収集の開始、停止の指示は、ログ収集装置１０５が接続している伝送路に，ログ収集の開始，停止の指示を含んだパケットを送ることにより行う。そして、ログ収集装置１０５の外部インタフェース制御部１１０４において、伝送路上の、このパケットを識別し，ネットワークアドレスによらずに、取り込むようにする。

【００５６】図１２に、このログ収集の開始，停止を指示に使用するパケットのフォーマットを示す。

【００５７】前述したようにパケットの第１フィールドはパケットの種別，第２フィールドは操作方法，第３フィールドは転送されるデータである。

【００５８】図１２（a）に示すように、ルータからログ収集装置に対してログ収集の開始を指示するパケットの、パケットの種別を示す第１フィールドには「ログ１２０１a」、操作方法を示す第２フィールドには「開始１２０２a」、転送されるデータである第３フィールドにはログ収集対象として指定する計算機のリスト１２０３aが設定される。また、図１２(b)に示すように、停止を指示するトラフィックログ収集停止パケットは、それぞれ「ログ１２０１b」、「停止１２０２b」、ログ収集対象から外される計算機リストである「ログ停止対象計算機リスト１２０３b」が設定される。

【００５９】ログ収集装置１０５は、自身が接続する伝送路上のパケットを監視し、第１フィールドにログが設定されたパケットについては，これを取り込み受信する。

11

【００６０】なお，以上の実施形態において、ネットワークへの接続前に計算機の内部ならびに外部監査を実施し、その結果に異常がないことをルータに通知しておかない限り、本ネットワークに計算機を接続しても信を開始することができないようルーが中継の内容を設定することもできる。また、計算機間で相互に外部監査を行うようにしてもよい。

【００６１】以上、本発明の一実施形態について説明した。

【００６２】本実施形態によれば、

(1)随時、管理装置からルータ、計算機が実行する監査プログラムを最新の監査プログラムに更新できる。

【００６３】(2)内部ならびに外部監査プログラムによる計算機の稼動環境を監査を行い、監査結果に異常がある場合には、これを計算機管理者ならびにシステム全体を管理する管理者に通知するので、管理者などは、稼動環境に不整合がある計算機の早期発見と早期対策を実施することができる。

【００６４】(3)稼動環境に不整合がある計算機については，ログ収集装置においてトラフィックログの収集を行うので，アクセス状況の記録に基づいた外部からの不正アクセスの検証を行うことができる。

【００６５】(4)稼動環境に不整合が発生しているが、対策の実施されない計算機については、ルータで該当計算機宛データの中継の停止を実施することにより、当該計算機への不正な侵入を排除し、ネットワークならびに計算機セキュリティを向上することができる。

【００６６】(5)ログ収集装置は、本ログ収集装置を明示的に宛先指定してメッセージを送信することはできないという機能を持つため、ネットワークを介してログ収集装置に格納されたログ情報の改竄や破壊を防ぐことができる。

【００６７】

【発明の効果】以上のように，本発明によれば、大規模

12

なネットワークを対象とした計算機の監査システムを提供することができる。また、計算機の稼動環境に不整合がある場合には、稼動環境の不整合を持つ計算機への不正な侵入を防止することができる。

【図面の簡単な説明】

【図１】ネットワークの構成を示す図である。

【図２】ルータ、計算機，ログ収集装置，管理装置のハードウェア構成例を示すブロック図である。

【図３】ルータのソフトウェア構成を示すブロック図である。

【図４】計算機のソフトウェア構成を示すブロック図である。

【図５】管理装置のソフトウェア構成を示すブロック図である。

【図６】ログ収集装置のソフトウェア構成を示すブロック図である。

【図７】監査プログラムの配布シーケンスを示す図である。

【図８】外部よりの監査の動作のシーケンスを示す図である。

【図９】内部よりの監査の動作のシーケンスを示す図である。

【図１０】監査に用いるパケットの内容を示す図である。

【図１１】ルータの行う動作を示すフローチャートである。

【図１２】ログ収集の開始／停止」指示に用いるパケットの内容を示す図である。

【符号の説明】

１０３　管理装置

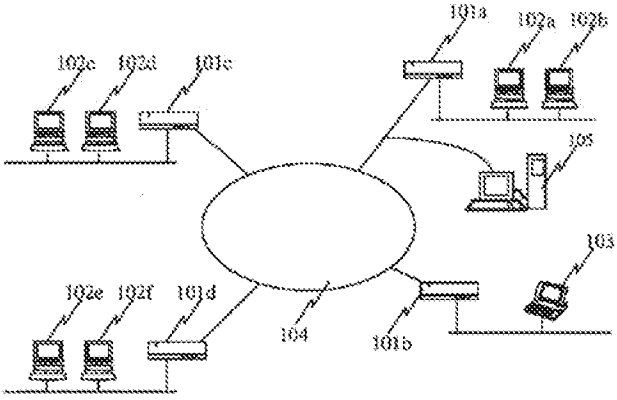
１０１ａ～１０１ｄ　中継装置

１０２ａ～１０２ｆ　計算機

１０５　ログ収集装置

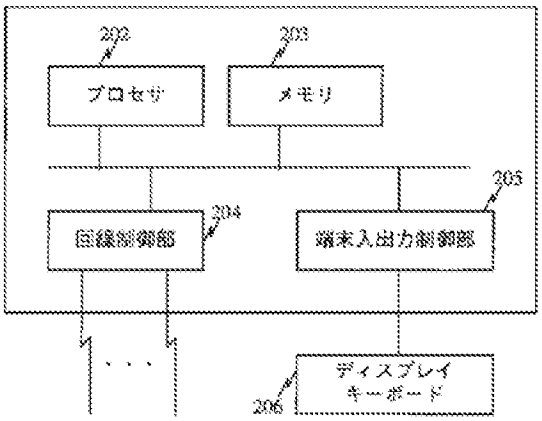
【図１】

図１



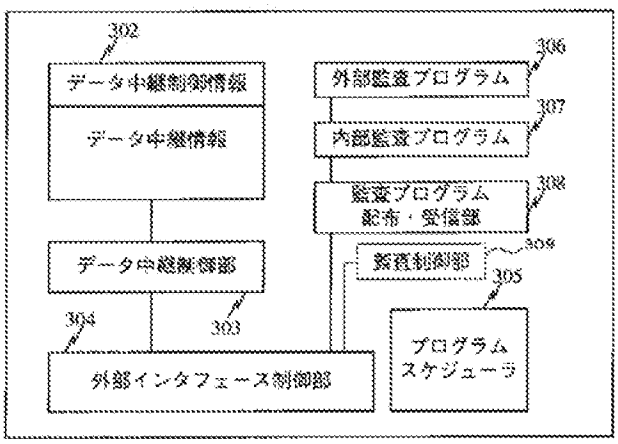
【図2】

図2



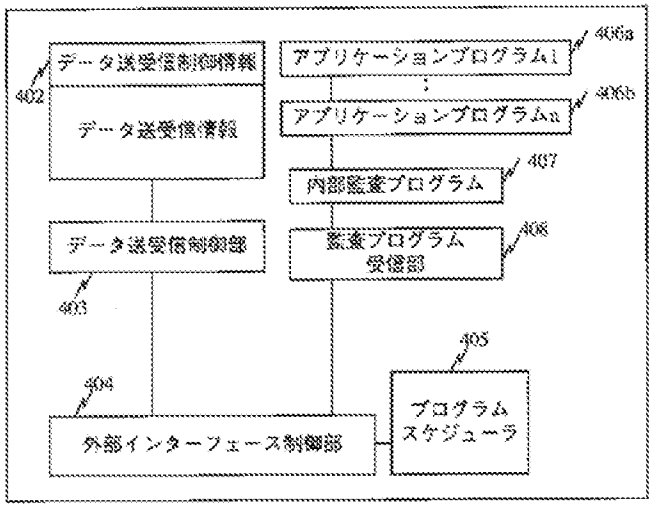
【図3】

図3



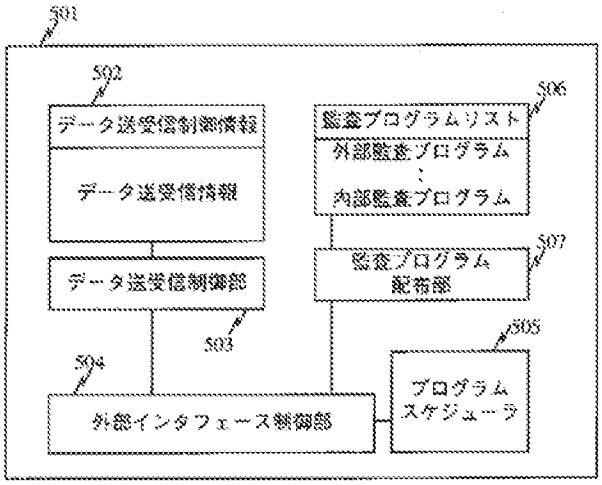
【図4】

図4



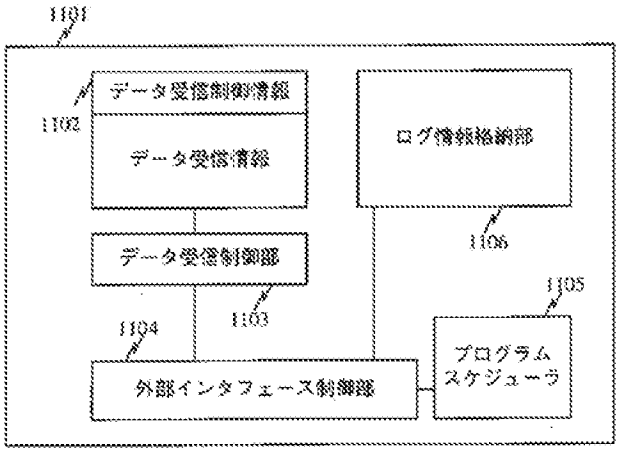
【図5】

図5



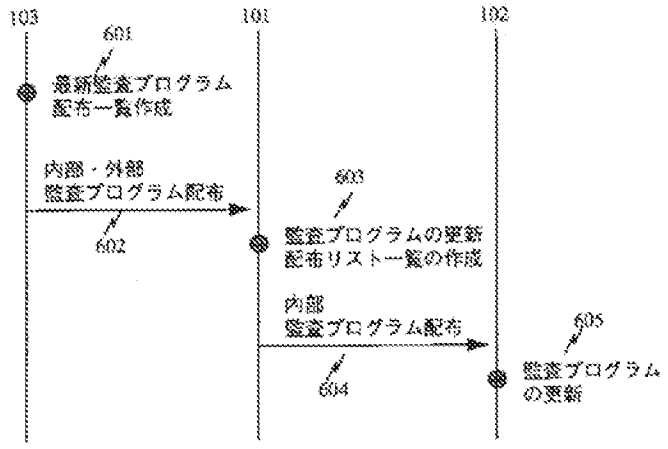
【図6】

図6



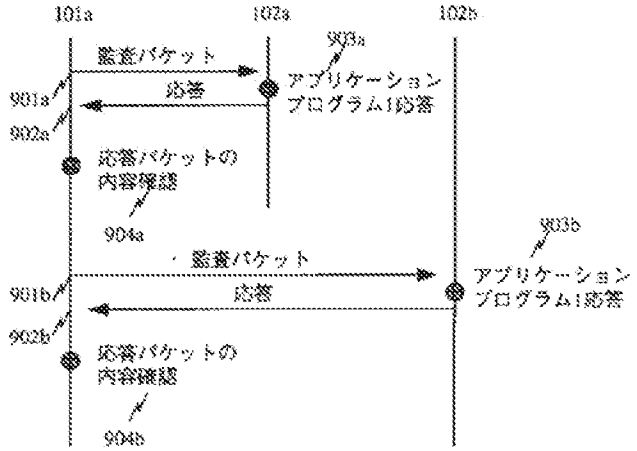
【図7】

図7



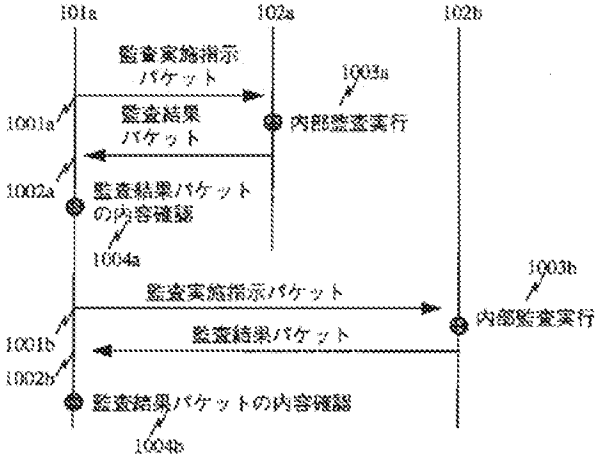
【図８】

図8


101a
102a
102b
903a
監査パケット
応答
アプリケーション
プログラム1応答
901a
902a
応答パケットの
内容確認
904a
903b
監査パケット
アプリケーション
プログラム1応答
901b
応答
902b
応答パケットの
内容確認
904b

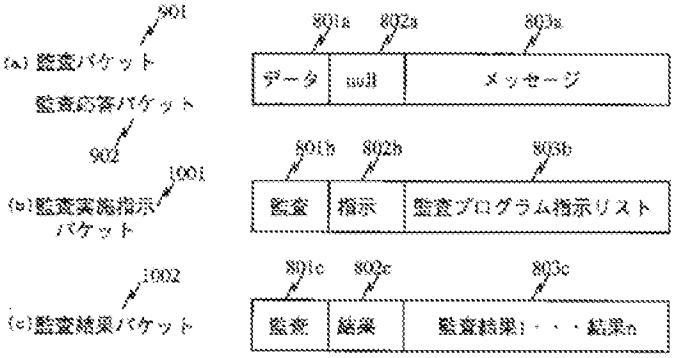
【図９】

図9


101a
102a
102b
監査実施指示
パケット
1003a
監査結果
パケット
内部監査実行
1001a
1002a
監査結果パケット
の内容確認
1004a
1003b
監査実施指示パケット
内部監査実行
監査結果パケット
1001b
1002b
監査結果パケットの内容確認
1004b

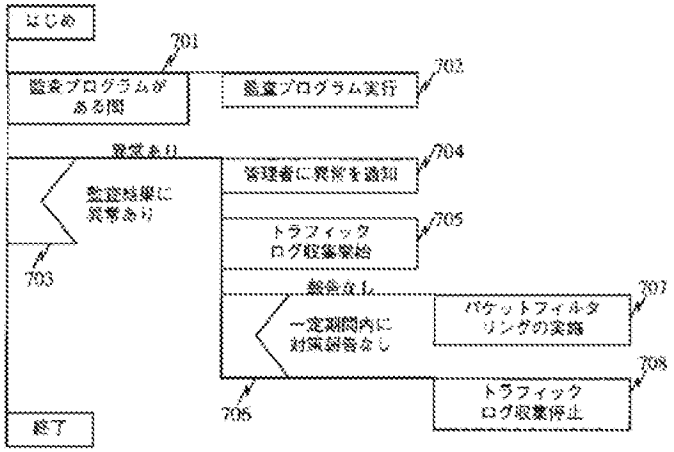
【図１０】

図10



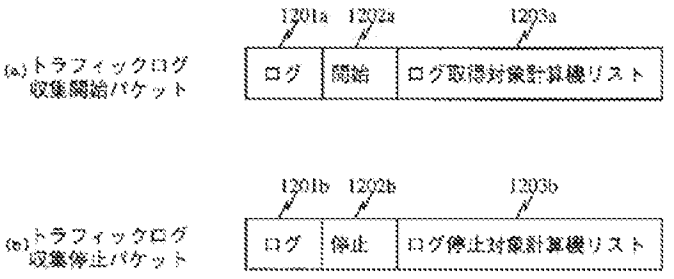
【図１１】

図11



【図１２】

図12



フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI		技術表示箇所
G06F	15/00	320		G06F	15/00	330A
		330	9466-5K	H04L	11/20	102Z
H04L	12/56					